Electronic Version
Stylesheet Version v1.1.1

Claims

[c1] A method for enabling strong mutual authentication on a computer network comprising the steps of:
transmitting, by a first computer, a first encrypted message to a second computer over a first communication channel; and
transmitting, by said first computer, a second message to said second computer over a second communication channel, wherein said second message comprises a second authentication number used to decrypt said first message.

[c2] The method of claim 1, wherein said first message comprises a first authentication number.

[c3] The method of claim 2, wherein said first authentication number is encrypted by said second authentication number.

[c4] The method of claim 1 further comprising transmitting a first indicia to said first computer over said first communication channel.

[c5] The method of claim 1 further comprising generating, by said first computer, at least one of said first authentica-

tion number and said second authentication number.

[c6] The method of claim 1 further comprising generating, by said first computer, a third authentication number.

[c7] The method of claim 1 further comprising transmitting, by said first computer, said second message to a verifier over said second communication channel and transmitting by said verifier said second message to said second computer over said second communication channel, wherein said second message comprises said second authentication number encrypted.

[c8] The method of claim 1, wherein said second communication channel further comprises a third communication channel.

[c9] The method of claim 1, wherein said second message further comprises a third authentication number.

[c10] The method of claim 7 further comprising decrypting, by said verifier, said second message to obtain a first decrypted message, wherein said first decrypted message comprises said second authentication number.

[c11] The method of claim 7, wherein said transmitting said second message to said second computer over said second communication channel further comprises transmit-

ting, by said verifier, said second authentication number to said second computer over said second communication channel.

[c12] The method of claim 1 further comprising decrypting, by said second computer, said first message transmitted by said first computer to recover said first authentication number.

[c13] The method of claim 1 further comprising transmitting, by said second computer, a third message to said first computer over said first communication channel, wherein said third message comprises said second authentication number encrypted by said first authentication number.

[c14] The method of claim 2 further comprising validating said second computer by said first computer by decrypting said third message to obtain said second authentication number.

[c15] The method of claim 1, wherein said second message further comprises an encrypted portion.

[c16] A system for enabling strong mutual authentication comprising:
a first transmitter; and
a first receiver in communication with said first transmit-

ter over a first communication channel and in communication with said first transmitter over a second communication channel;
wherein said first transmitter transmits a first encrypted message to said first receiver over said first communication channel; and
wherein said first transmitter transmits a second message to said first receiver over said second communication channel, sdaid second message used to decrypt said first encrypted message.

[c17] The system of claim 16 further comprising:
a second transmitter; and
a second receiver in communication with said second transmitter over said first communication channel;
wherein said second transmitter transmits a first indicia to said second receiver over said first communication channel,
wherein said second transmitter transmits a third message to said second receiver over
said first communication channel, said third message comprising at least a portion of said decrypted first encrypted message.

[c18] The system of claim 17 further comprising a comparator in communication with said first transmitter and said second receiver to compare at least a portion of said

third message with at least a portion of said decrypted first encrypted message.

[c19] The system of claim 16, wherein said second message is encrypted.

[c20] The system of claim 19 further comprising a verifier in communication with said first transmitter to decrypt said encrypted second message to obtain a key to decrypt said first encrypted message.

[c21] An apparatus for enabling strong mutual authentication on a computer network comprising:
means for transmitting a first message to a computer over a first communication channel, wherein said first message comprises a first encrypted authentication number; and
means for transmitting a second message to said computer over a second communication channel, wherein said second message comprises a second authentication number used to decrypt said first message.

[c22] The apparatus of claim 21 wherein said first encrypted authentication number is
encrypted by said second authentication number.

[c23] A method for enabling strong mutual authentication on a computer network comprising the steps of:

transmitting, by a server computer, a first encrypted message to a client computer over a first communication channel;

receiving, by said client computer, a key over a second communication channel; and

transmitting, by said client computer, a decrypted message over said first communication channel.